International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

HIGH PERFORMANCE OF AES USING XOR BASED MIXED COLUMN

Shilparani[1], Dr.G S Biradar[2]

[1]Student, ECE Department, VTU RC Gulbarga, Karnataka, India
[2] Professor, ECE Department, PDACE Gulbarga, Karnataka, India

Abstract: **Increasing need of data protection in computer networks led to the development of several cryptographic algorithms hence sending data securely over a transmission link is critically important in many applications. Implementation of cryptographic algorithms are physically secure than software implementations since outside attackers cannot modify them. In order to achieve higher performance in today's heavily loaded communication networks, hardware implementation is a wise choice in terms of better speed and reliability. The details compact and flexible architectures for mix column applied to the AES.This paper presents the hardware implementation of Advanced Encryption Standard (AES) algorithm using Xilinx–virtex5 Field Programmable Gate Array (FPGA). In order to achieve higher speed and lesser area, Sub Byte operation, Inverse Sub Byte operation, Mix Column operation and Inverse Mix Column operations are designed as Look Up Tables (LUTs) and Read Only Memories (ROMs). This approach gives a throughput of 3.74Gbps utilizing only 1% of total slices in xc5vlx110t-3-ff1136 target device.**

Key Words: **AES, Rijndael, Cryptography, FPGA, Verilog, Encryption, Decryption.**

1. INTRODUCTION

Cryptography allows people to carry over the confidence found in the physical world to the electronic world. The importance of cryptography is constantly increasing since the amount of sensitive data being transmitted over an open environment is also increasing day by day. The more information that is transmitted in computer-readable form, the more vulnerable we become to automated spying. Cryptography is not only important in defense applications but also important in real world applications such as E-commerce, E-mail etc. Encryption is usually done just before sending data. To utilize the channel resources completely encryption algorithm must have a speed at least equivalent to data transmission speed. Achieving high throughput for encryption algorithm for a communication channel of high data rate is a challenging task. The hardware (FPGAs and Application Specific Integrated Circuits-ASICs) implementation of such algorithm which meets these requirements is done in the present work. FPGAs are chosen considering several advantages over the other counterpart [1].

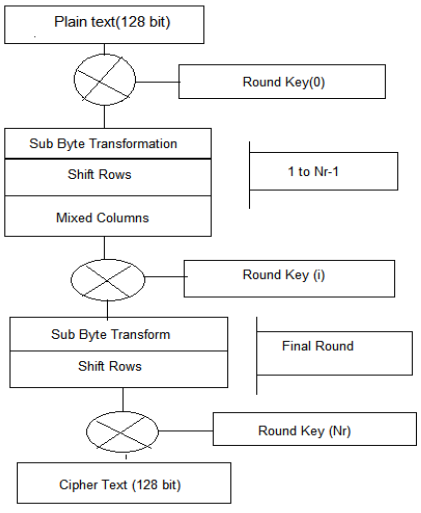
The AES was published by National Institute of Standards and Technology (NIST) in 2001. Later Rijndael algorithm was selected as AES algorithm. Rijndael algorithm can have key length of 128, 192 and 256 bits while block size must be 128bit [2]. There are many architecture proposals for AES Rijndael algorithm [3, 4], but many of them are poor in terms of area and speed. This paper proposes a different approach to increase speed by utilizing lesser resources available in FPGA

2. AES ALGORITHM

The AES is a computer security standard from NIST intended for protecting electronic data. Federal Information AES use Rijndael algorithm [5] by Joan Daeman and Vicent Rijimen for both encryption and decryption. The AES cryptography algorithm is capable of encrypting and decrypting 128 bit data using cipher keys of 128, 196 or 256.

Rijndael encryption consist of four operations

1. Substitution
2. Shift Row
3. Mix Column
4. Key Addition.



Algorithm for AES Encryption

The Rijandael decryption consists of four inverse operations of encryption which are compliment functions of encryption. They are

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

1. Inverse Substitution
2. Inverse Shift Row
3. Inverse Mix Column
4. Key addition

2.2 Sub Byte and Inverse Sub Byte transformation

In the Sub Bytes step, each byte in the *state* matrix is replaced with a Sub Byte using an 8-bit data from the Rijndael S-Box. In the Inverse Sub Bytes step, each byte in the *cipher* matrix is replaced with corresponding Inverse Sub Byte. Sub Byte operation provides the non-linearity in the cipher. The SBox used is derived from the multiplicative inverse over Galois Field (28) [7], known to have good non-linearity properties. Many S-Box implementation [7] use combinational circuit consists of an adder, squarer and constant multiplier. Rijndael S-Box is not shown for brevity.

2.3 Shift Row Transformation

The Shift Rows transformation cyclically shifts the bytes in each row by certain offset to the left. For AES, the first row is left unchanged. Each byte of the second row is shifted by one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Inverse Shift Row transformation does the same shift operation towards right.

2.4 *Mix Column and Inverse Mix Column operation*

In the Mix Column step, the four bytes of each column of the state are combined using an invertible linear transformation. All entries in the state matrix are considered tobe a polynomial and it is multiplied by a fixed polynomial. The Mix Column and inverse Mix Column transformation are represented in matrix form. Where cij and dij are Mix Column input and Output respectively, while aij and bij are respectively the inputs and outputs of Inverse Mix Column operation.

2.5 *Add Round Key operation*

In this operation, bitwise exclusive-or (XOR) operation is performed between outputs from Mix Column and Round Key. For AES-128, 128 bit XOR operations are performed.

3. PROPOSED WORK

The proposed architecture is designed to get maximum speed and lesser area by mapping all the four Logical functions of AES to LUTs, ROMs and Block RAMs.
The proposed architecture has three parts

1. Key Generation Module
2. Encryption Module
3. Decryption Module.

The AES encryption and decryption core unit contains key generation module as a common unit. This module gives necessary key expansion for both encryption and decryption functions. Encryption and decryption with Key Generation Module as a common unit. The key generation module consists of key register of 128 bits, S-Box and XOR gates for bitwise XOR operation.

It is designed to produce round keys on each positive edge of the clock, when it is enabled. However in the proposed work, the key generation architecture does not require any hardware for shift operation and the port mapping between key register and S-Box is done according to the required shift. Hence the proposed work offers the advantage in area. Also in the proposed work the bits are rearranged on data path from register to S-Box and the round constant required for each rounds are stored in ROM and retrieved on each clock. Fig represents proposed architecture of key generation unit.

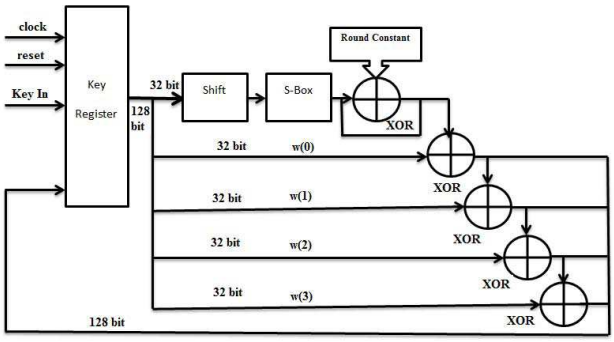


Fig: Architecture of Key Generation Module

The encryption module takes 128 bit text to be encrypted and receives round key from key generation module to do each round of encryption. Fig. presents the proposed encryption module

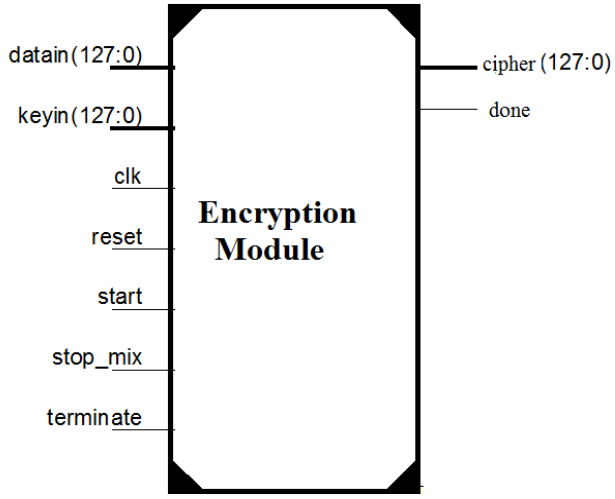


Fig: Encryption module

In the proposed work for reducing the hardware of entire architecture, the control unit of encryption module is no

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

designed separately. The control unit of key generation module which is a 4-bit counter is designed to control the entire functioning of encryption module. The sharing of control unit by both encryption and round key generation gives unique advantage of reduction in hardware as compared to other implementations

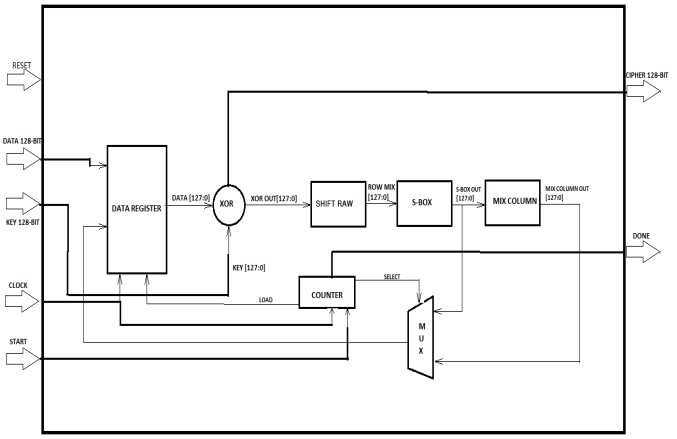


Fig: Proposed Architecture of Encryption Module

NAND gate and the 4-bit counter (Controller) are used to set and reset selection line of Multiplexer. For count one to ten the selection line will be in set condition and multiplexer will pass Mix Column output. However on last round, count will be eleven so selection line will reset and pass Sub Byte output. Shift Row operation is designed in such a way that it does not take any hardware. After Round Key operation data is given to S-Box with required shift by port mapping the signal according to required shift in Verilog HDL description of the design. Since there is no hardware for Shift Row operation design gets the advantage of area, power and speed.

In the proposed work, the S-Box is implemented by a LUT having 8 bit address (256 addresses) and a data width of 8 bit. This implementation gives higher throughput for the design by significantly decreasing delay in data path. As a result the proposed design takes lesser number of slices when compared with other combinational technique proposed in [7]. The Mix Column operation of AES consists of Galois multiplication and four input XOR operation. But unlike combinational implementation [8] of Galois field multiplication, the proposed design uses ROM based implementation of Galois multiplication which makes Galois multiplication significantly faster avoiding combinational delays. For an 8-bit data there are 256 multiplication conditions and all the conditions are stored in (256 x 8) ROM. In the proposed work the Mix Column encryption hardware uses two of such ROM for Galois multiplication of '2' and '3' and for performing 4-Input XOR operation in Mix Column operation, the proposed design use 16 x 1 ROM with the result that Mix Column operation offers higher speed and uses minimum number of slices in the hardware (FPGA). The decryption unit also uses same design approach for the entire architecture and takes 20 clock cycles to decrypt the given cipher back to original text. Inverse S-Box architecture uses the same design of S-Box. Entry of LUT is changed according to Inverse Sub Byte transformation. Mix Column operation is implemented using 256X8 ROM. Four such ROMs are designed for the Galois multiplication of 9, 11, 13 and 14. 4-Input XOR operation is designed by 16x1 ROM. Architecture of Decryption module is same as encryption module with all complimentary functions of encryption. Decryption unit contains an extra register for storing Round Keys. Storing key is important since first round decryption use tenth round key and second round use ninth round key and so on. Count register is synthesized as B-Ram to save number of slices. 'Count' input provides the address of key register location to be accessed. The Architecture of decryption module is shown in Fig

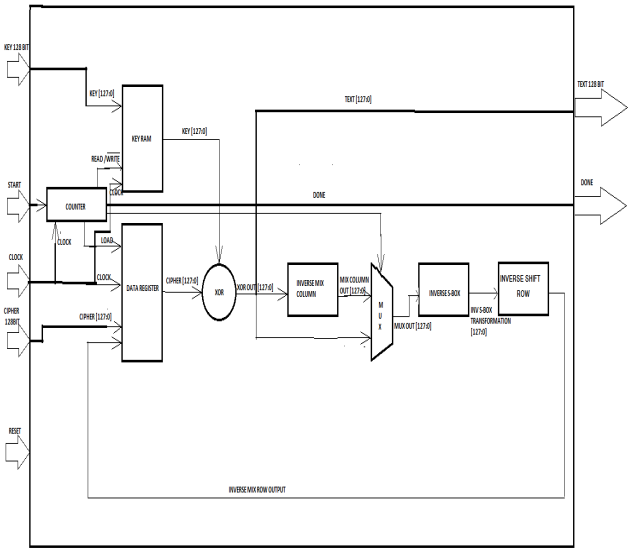


Fig: Proposed Architecture of Decryption Module

4. SIMULATION RESULTS

AES Rijndael algorithm is simulated and synthesized using Xilinx 12.1 ISE tool and the targeted FPGA is 5vlx110tff1136-3 which belongs to Virtex-5 family. The design uses only LUTs, ROMs for all the operations of AES encryption and decryption. This approach reduces device utilization and significantly improves the speed compared to other implementation [3,4,9]. The key register in the decryption module is synthesized as Block-Ram to reduce the number of slices used. The utilization summary for device 5vlx110tff1136-3In this proposed design, the encryption unit takes 10 clock cycles to complete the operation. The maximum path delay of the design is 3.420ns resulting in a maximum frequency of operation as 292.403MHz. The throughput of the proposed encryption module is 3.74Gbps

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

5. CONCLUSION

AES-128 algorithm for encryption and decryption is implemented in Virtex-5 FPGA. With the designing of all the operations as LUTs and ROMs, the proposed architecture achieves a throughput of 3.74 Gbps and thereby utilizing only 1% of slices in the targeted FPGA. Since the speed is higher than the already reported systems, hence the proposed design serves as the best high speed encryption algorithm and is thus suitable for various applications. Moreover with less area utilization, the proposed design can be embedded with other larger designs as well.using XOR based mix columns.

REFERENCE

[1]. M. Goswami and S. Kannojiya, "High Performance FPGA Implementation of AES Algorithm with 128-Bit Keys," Proc. IEEE Int. Conf. Advances Computing Comm., vol. 1, Himarpur, India, 2011, pp. 281-286.
[2]. FIPS-197, NIST - National Institute of Standards and Technology, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.
[3]. W. Wei, C. Jie and X. Fei, "An Implementation of AES Algorithm on FPGA," IEEE 9th Int. Conf. on Fuzzy Systems and Knowledge discover 2012, pp. 1615-1617.
[4]. U. Kretzschmar, A. Astarloa, J. Lazaro, U. Bidarte and J. Jimenez, Robustness analysis of different AES implementations on SRAM based FPGAs," Int. Conf. on Reconfigurable Computing and FPGAs 2011, pp. 255-260.
[5]. J. Daeme and V. Rijmen, "AES proposal: Rijndael," NIST AES Proposal, June 1998.
[6]. Stallings, "Cryptography and network security principles and practice," Pearson edition 2009, pp. 135-160.
[7]. V.S. Shastry, A. Agnihotri, D. Kachhwaha, J. Singh and M.S. Sutaone, "A Combinational Logic Implementation of S-Box of AES," IEEE 54th Int. Midwest Symp. on Circuits and Systems (MWSCAS), Aug. 2011, pp. 1-4
[8]. S. Kaur and R. Vig, "Efficient Implementation of AES Algorithm in FPGA Device," Int. Conf. on Computational Intelligence and Multimedia Applications, Dec. 2007, pp. 179 – 187.
[9]. H. Trang and N.V. Loi, "An efficient FPGA implementation of the Advanced Encryption Standard algorithm," IEEE Int. Conf. on Computing and Communication Technologies, Research, Innovation and Vision for the Future (RIVF), 2012, pp. 1-4.